

UNITED STATES DISTRICT COURT

for the
Eastern District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)A Macbook Pro computer utilized by
Kevin Patrick Mallory

Case No. 1:17sw

354

JUN 21 2017
UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A Macbook Pro computer utilized by Kevin Patrick Mallory.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 793	Gathering, transmitting or losing defense information
18 U.S.C. § 794	Gathering or delivering defense information to aid a foreign government
18 U.S.C. § 1956	Laundering of monetary instruments

The application is based on these facts:

See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA John T. Gibbs

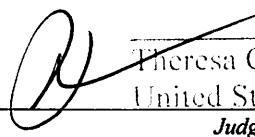


Applicant's signature

Stephen Green, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 06/21/2017 /s/ Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Theresa C. Buchanan, U.S. Magistrate Judge

Printed name and title

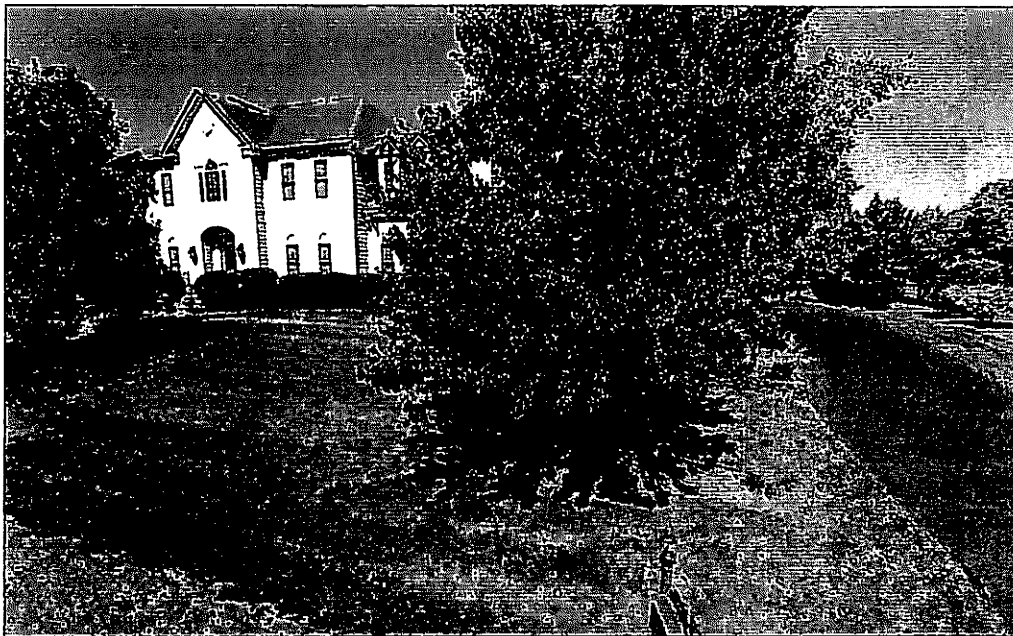
ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The PREMISES to be searched is:

KEVIN PATRICK MALLORY's residence, located at 16621 Elk Run Court, Leesburg, VA 20176. The residence is a two-story single family house in a residential neighborhood. The residence has two red banners, containing writing in Mandarin, hanging on either side of the front door.

Mallory is self-employed with GlobalEx, LLC, a business registered to 16621 Elk Run Court, Leesburg, VA 20176.





ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956, including:

1. Notebooks or documents, records, or papers containing information relating to the national defense and/or classified information;
 2. Notebooks or documents, records, or papers containing U.S. Government information;
 3. Information pertaining to any recipients of classified information, including information pertaining to their identity, location, their communications with Kevin Patrick Mallory, financial transactions related to the receipt of classified information, data exchange with or between such persons, and photographs of such persons;
 4. Information regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
 5. Records of travel, including calendars, travel tickets, receipts, and photographs;
 6. Information pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;
 7. Computer hardware, computer software, passwords and data security devices, cameras (including digital and video), telephones, handheld devices, computer related documentation, and other digital and electronic media, including storage devices that may have been used to store or transmit classified information;
 8. Records or documents evidencing ownership or use of computer hardware, computer software, telephones, cameras, handheld devices, electronic media and electronic storage devices, including sales receipts, bills for Internet access, and handwritten notes;
 9. Financial records, including bank statements, account information and records of any financial transaction, as well as any currency, including U.S. currency, that may be evidence of payments for the sale of classified information;
 10. Miscellaneous papers, magazines, books, or any other pocket litter, especially that which may contain handwriting, computer-generated text or highlighted sections.
 11. Items containing potential passwords or passphrases.
-

SEARCH PROCEDURE

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

1. On-site search, if practicable. Law enforcement officers training in computer forensics (hereafter computer personnel), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.
2. On-site imaging, if practicable. If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.
3. Seizure of digital devices for off-site imaging and search. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.
4. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.
5. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.
6. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

7. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.
8. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNDER SEAL

IN RE: SEARCH WARRANTS
INVOLVING KEVIN MALLORY

)
)
)

CASE NO. 1:17 sw-354

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Stephen Green, after being duly sworn, depose and state as follows:

1. I am a Special Agent with the FBI, and have been since 2012. Since 2012, I have been assigned to the Washington Field Office, Counterintelligence Division. Since October 2016, I have investigated offenses involving espionage and the unlawful retention or disclosure of classified information. I was the affiant on the affidavit in support of a criminal complaint and arrest warrant, charging Kevin Patrick Mallory (hereinafter Mallory) with making materially false statements to Federal Bureau of Investigation (FBI) agents, in violation of 18 U.S.C. § 1001, and Gathering or Delivering Defense Information to Aid a Foreign Government, in violation of 18 U.S.C. § 794. I adopt the facts contained in that affidavit ("the Criminal Complaint Affidavit") as true statements for this affidavit and incorporate them here.

2. This affidavit is submitted in support of an application to search the following locations or things:

- a. Mallory's residence at 16621 Elk Run Court, Leesburg, Virginia 20176;
- b. The vehicle identified by VIN 4T1BF12B2TU073343 which is registered at Mallory's residence;
- c. The vehicle identified by VIN JT6HT00W9Y0084109 which is registered at Mallory's residence;

- d. One Apple iPhone 5 phone utilized by Mallory;
- e. One Apple iPhone 7 utilized by Mallory;
- f. One Samsung Galaxy cell phone utilized by Mallory;
- g. One Macbook Pro computer utilized by Mallory.

3. Based on the facts set forth in this affidavit (and incorporating the facts contained in the Criminal Complaint Affidavit), there is probable cause that within these locations or things is evidence, more particularly described in Attachment A, of violations of federal law, including 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956.

4. This affidavit is being submitted for the limited purpose of obtaining a search warrant. As a result, it does not include each and every fact observed by me or known to the government. When I assert that a statement was made by an individual, that statement is described in substance and in part, but my assertion is not intended to constitute a verbatim recitation of the entire statement. When I assert that an event occurred or a communication was made on a certain date, I mean that the event occurred or the communication was made “on or about” that date.

5. In addition to the information contained in the Criminal Complaint Affidavit, I bring to the Court’s attention the following:

Additional Statutory Authority and Definitions

6. Under 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted” or attempts to do or causes the same “to any

person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

7. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

8. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled “Storage,” regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information “shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53.” It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

9. Under 18 U.S.C. § 1956(a)(2), “Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States (A) with the intent to promote the carrying on of specified unlawful activity; or (B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or (ii) to avoid a transaction reporting requirement

under State or Federal law, shall be sentenced to a fine of not more than \$500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both.”

Mallory Resides at 16621 Elk Run Court, Leesburg, Virginia 20176

10. Mallory’s current driver’s license, valid from March 16, 2012 through April 8, 2020, issued by the state of Florida, lists Mallory’s address as 16621 Elk Run Court, Leesburg, Virginia 20176. Mallory is self-employed with GlobalEx, LLC, a business registered to 16621 Elk Run Court, Leesburg, Virginia 20176. During an interview with Customs and Border Protection (“CBP”) on April 21, 2017, following a trip that he had taken to Shanghai, China, Mallory provided his address as 16621 Elk Run Court, Leesburg, Virginia 20176.

Mallory Utilizes Vehicles DTTD71 and EJAW81

11. According to the records of the Florida Department of Motor Vehicles, as of June 7, 2017, Kevin Patrick Mallory, of 16621 Elk Run Ct, Leesburg, Virginia 20176, was the registered owner of one 1996 blue Toyota, bearing Vehicle Identification Number 4T1BF12B2TU073343, and Florida license tags DTTD71. On April 1, 2017, the FBI observed DTTD71 parked and unoccupied in front of 16621 Elk Run Court, Leesburg, Virginia. At or around 11:10am on April 1, 2017, Mallory entered DTTD71 and drove east on Harry Byrd Highway (Route 7).

12. According to the records of the Florida Department of Motor Vehicles, as of June 6, 2017, Nan Hua Mallory, of 16621 Elk Run Ct, Leesburg, Virginia 20176, was the registered owner of one white Lexus, bearing Vehicle Identification Number JT6HT00W9Y0084109, and Florida license tags EJAW81. Multiple instances of physical surveillance in March 2017 and April 2017 observed a Lexus SUV, bearing Florida license tags EJAW81, parked at Mallory’s

primary residence, 16621 Elk Run Court, Leesburg, Virginia. On April 3, 2017, Mallory was observed as a passenger in EJA81. On April 17, 2017, Mallory was observed driving EJA81.

Mallory utilizes Apple and Samsung cell phones

13. On April 21, 2017, on a return flight to the United States from Shanghai, China, Mallory was subject to a CBP secondary search and interview by CBP Agents at Chicago O'Hare Airport. Mallory was informed that CBP policy and procedure dictated that anyone crossing the border was subject to inspection, including an inspection of all of their belongings and electronic devices. At that point, Mallory turned over his Apple iPhone 5, which he claimed to have had for 4-5 years, and his Apple iPhone 7, which he claimed to have had for 3-4 months. Mallory stated that he had purchased a new MacBook pro and a brand new Samsung Galaxy phone during his trip to China.

14. On May 24, 2017, in an interview with FBI Agents, Mallory had in his possession an Apple iPhone 7, an Apple iPhone 5, and a Samsung Galaxy phone. Mallory informed agents these were all his phones which he utilized to communicate for various purposes.

Evidence Is Likely to be Found in the Residence

15. Based on my knowledge, training and experience, as well as that of other agents assigned to this investigation from the FBI, I know that individuals generally keep important documents and financial records in their home or office. Mallory is self-employed at a business registered to his home address, and I believe that his residence is the location in which he keeps his important records. In fact, this investigation has revealed that the only location where Mallory is known to have an office is in his home. Moreover, during an interview with the FBI lasting nearly three hours on May 24, 2017, Mallory talked about his consulting business,

GlobalEx, yet he never claimed to have a different location for that business, other than his home.

16. Based on this investigation, I know that Mallory has transmitted documents classified at the TOP SECRET and at the SECRET level to an individual in the People's Republic of China ("PRC") that he believes is an agent of the government of the PRC. These documents constitute national defense information. Given that Mallory previously worked at the U.S. government agency that classified these documents, and given that these documents are several years old, I believe that it is likely that Mallory maintains these documents and/or other similar documents in his home, especially because he has communicated to the PRC government agent about his desire to sell him/her additional documents like the ones previously provided. For example, on May 5, 2017, in a communication with this PRC government agent ("PRC1"), he stated, "I can also come in the middle of June. I can bring *the remainder of the documents I have* at that time." (Emphasis added). These records may include documents, records, or papers containing information relating to the national defense and/or classified information which Mallory may have retained and passed to a foreign government. Such records are also likely to reveal any others who conspired with Mallory to release, communicate, or transmit national defense information and/or classified information.

17. Based on my knowledge, training and experience, as well as that of other agents assigned to this investigation from the FBI, I know that important records are often maintained in hard copy and/or digital form, such as on computers and other electronic devices. This application seeks permission to search and seize records that might be found in Mallory's residence, vehicles, and cellular phones, in whatever form they are found. One form in which records might be found is stored on the hard drive or other storage media of a computer or other

electronic device. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

18. I know that Mallory uses electronic devices and is sophisticated about computer matters. As described in the Criminal Complaint Affidavit, Mallory has training in counter-intelligence “tradecraft,” and has utilized multiple communication devices and multiple communication methods with PRC1. Additionally, in a message on May 3, 2017, Mallory told PRC1, “If they we looking for me in terms of State Secrets, and found the sd card..., we would not be talking today. I am taking the real risk....” Based on my training and experience, this indicates that Mallory used a different electronic device (which could include a Samsung Galaxy phone, a MacBook Pro computer, or some other device) to transmit the classified documents onto one or more SD cards. The SD card(s) could be used to store and, ultimately, transfer documents onto various electronic devices for storage or potential transmission of the documents to the PRC.

19. Based on the information described above, Mallory is likely to use and maintain electronic media equipment. Based on my training and experience, he is likely to use and maintain such equipment, including cellular phones and his MacBook Pro computer, in his residence or in his or his wife’s vehicle. There is probable cause to believe evidence will be found in such electronic media for at least the following reasons:

a. As described in the Criminal Complaint Affidavit, when Mallory was interviewed by the FBI on May 24, 2017, he specifically admitted that PRC1, the person he believed was a PRC government agent, had given him a device to use for electronic communications between them. Mallory also described to the FBI how he had used

multiple electronic communication devices and methods to correspond with PRC1.

Based on this information, as well as my training and experience, I believe that it is likely that Mallory's Chinese contact will expect him to communicate with him/her through electronic media, and any electronic media belonging to Mallory will likely contain evidence of his communications with his Chinese contact. Also, it is likely that Mallory communicated with his Chinese contact on some other device(s) before he obtained the communications device from PRC1. Since the FBI is aware that Mallory has two Apple iPhones, a Samsung Galaxy cell phone and a MacBook Pro computer, it is likely that those earlier communications will be found on one or more of those devices, or on some other device belonging to Mallory of which the FBI is unaware.

b. Based on my knowledge and training, I know that computer files or remnants of computer files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

20. In light of these concerns, I request authority to seize the computer hardware, storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence. I further seek authority to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when.

21. Based on the visit of FBI agents to Mallory's residence in March 2017, I know that the residence at 16621 Elk Run Court, Leesburg, Virginia 20176 is a two-story single family

house in a residential neighborhood. The residence has two red banners, containing writing in Mandarin, hanging on either side of the front door. To the left of the door are affixed the numbers “16621.”


Conclusion

22. Based on the foregoing (and incorporating the information in the Criminal Complaint Affidavit), there is probable cause to believe that evidence of violations of federal law, including 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956, more particularly described in Attachment A, will be found in the following locations and things:

- a. Mallory’s residence at 16621 Elk Run Court, Leesburg, Virginia 20176;
- b. The vehicle identified by VIN 4T1BF12B2TU073343 which is registered at Mallory’s residence;
- c. The vehicle identified by VIN JT6HT00W9Y0084109 which is registered at Mallory’s residence;
- d. One Apple iPhone 7 utilized by Mallory;
- e. One Apple iPhone 5 utilized by Mallory;
- f. One Samsung Galaxy cell phone utilized by Mallory;
- g. One MacBook Pro computer utilized by Mallory.

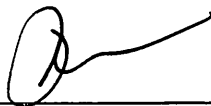
Wherefore, I request the issuance of a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

FURTHER THIS AFFIANT SAYETH NOT.



Stephen Green
Special Agent
Federal Bureau of Investigation
Washington, D.C.

Subscribed and sworn to before me
on June 21, 2017.



/s/
Theresa Carroll Buchanan
United States Magistrate Judge

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The PREMISES to be searched is:

KEVIN PATRICK MALLORY's residence, located at 16621 Elk Run Court, Leesburg, VA 20176. The residence is a two-story single family house in a residential neighborhood. The residence has two red banners, containing writing in Mandarin, hanging on either side of the front door.

Mallory is self-employed with GlobalEx, LLC, a business registered to 16621 Elk Run Court, Leesburg, VA 20176.





ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. § 793(e), 18 U.S.C. § 794(a), and 18 U.S.C. § 1956, including:

1. Notebooks or documents, records, or papers containing information relating to the national defense and/or classified information;
 2. Notebooks or documents, records, or papers containing U.S. Government information;
 3. Information pertaining to any recipients of classified information, including information pertaining to their identity, location, their communications with Kevin Patrick Mallory, financial transactions related to the receipt of classified information, data exchange with or between such persons, and photographs of such persons;
 4. Information regarding tradecraft, how to obtain or deliver sensitive information, and/or how to avoid or evade detection by intelligence officials or law enforcement authorities;
 5. Records of travel, including calendars, travel tickets, receipts, and photographs;
 6. Information pertaining to any others who conspired with Kevin Patrick Mallory to release, communicate, or transmit national defense information and/or classified information;
 7. Computer hardware, computer software, passwords and data security devices, cameras (including digital and video), telephones, handheld devices, computer related documentation, and other digital and electronic media, including storage devices that may have been used to store or transmit classified information;
 8. Records or documents evidencing ownership or use of computer hardware, computer software, telephones, cameras, handheld devices, electronic media and electronic storage devices, including sales receipts, bills for Internet access, and handwritten notes;
 9. Financial records, including bank statements, account information and records of any financial transaction, as well as any currency, including U.S. currency, that may be evidence of payments for the sale of classified information;
 10. Miscellaneous papers, magazines, books, or any other pocket litter, especially that which may contain handwriting, computer-generated text or highlighted sections.
 11. Items containing potential passwords or passphrases.
-

SEARCH PROCEDURE

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

1. On-site search, if practicable. Law enforcement officers training in computer forensics (hereafter computer personnel), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.
2. On-site imaging, if practicable. If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.
3. Seizure of digital devices for off-site imaging and search. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.
4. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.
5. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.
6. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

7. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.
8. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.